УДК 004.056.5

ОСОБЕННОСТИ СБОРА СОБЫТИЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

Мешков А.В. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Попов И.Ю.
(ИТМО)

Введение. В современных информационных системах задачи целостности, конфиденциальности и доступности данных являются приоритетными. Способность качественно собирать и анализировать события безопасности операционной системы имеет ключевое значение для обнаружения потенциальных угроз и реагирования на них. В данном исследовании рассматриваются классические методы сбора событий безопасности операционной системы Windows и особенности, которые позволят увеличить эффективность данного процесса.

Основная часть. Использование стандартных настроек сбора событий безопасности операционной системы Windows [2] позволяет зафиксировать лишь часть потенциальных действий нарушителей информационной безопасности. Для увеличения объёма получаемых данных необходимо использовать расширенные настройки, специализированные дополнительные утилиты и решения для централизованной обработки событий безопасности.

Расширенные настройки аудита Windows [1] дают возможность фиксировать более широкий спектр событий безопасности, включая подробную информацию о действиях пользователей, доступе к файлам, системных изменениях и т.д. Например, включение аудита командной строки в событиях создания процесса позволяет отслеживать параметры запуска файлов, утилит, что повышает общую эффективность обнаружения угроз.

Специализированная дополнительная утилита Sysmon [3] является мощным инструментом для глубокого анализа потенциальных угроз и подозрительных действий нарушителя. Эффективность данного решения позволяет генерировать корреляционные события безопасности на основе разработанных правил мониторинга, указанных в конфигурации, в отдельный журнал. Это позволяет создать профиль злоумышленника и адаптировать сбор событий безопасности в соответствии с направлением и инфраструктурными особенностями организации.

Также существует класс решений, который позволяет администрировать и управлять потоками событий безопасности, фильтровать данные и помогает выявлять подозрительные действия в информационных системах – система мониторинга и управления информационной безопасностью (СМУИБ, SIEM). Данный класс решений позволяет централизованно собирать события безопасности с множества рабочих станций и серверов, создавать правила мониторинга и т.д.

Выводы. Проведен анализ методов сбора событий безопасности операционной системы Windows и определены их особенности.

Список использованных источников:

1. Advanced security audit policies [Электронный ресурс] / Microsoft Learn. — Режим доступа: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing (дата обращения: 14.02.2024).
2. Basic security audit policies [Электронный ресурс] / Microsoft Learn. — Режим доступа: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies (дата обращения: 14.02.2024).
3. Sysmon [Электронный ресурс] / Microsoft Learn. — Режим доступа: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon (дата обращения: 14.02.2024).